

Access Control Policy

How access to systems and data is granted, reviewed, and revoked on a least-privilege basis.

Version: 1.0 · Last updated: January 2026 · Owner: Security Lead

1. Purpose

To ensure access to systems and data is granted on a least-privilege, need-to-know basis and removed when no longer required.

2. Scope

The Backpack OS platform, internal systems, cloud environments, and client environments accessed by Backpack Works personnel and customers.

3. Principles

- **Least privilege.** Users receive the minimum access required for their role.
- **Tenant isolation.** In Backpack OS, every record is scoped to an organization and enforced at the database layer with PostgreSQL Row-Level Security (RLS); users can only access data for organizations they belong to.
- **Privilege separation.** User requests use a least-privilege, RLS-respecting database client; a separate elevated service-role client is used only by trusted server-side jobs and is never exposed to the browser.
- **Role-based access (RBAC).** Platform roles (e.g. admin, project owner, contributor; client vs. team visibility) gate features and data. Sensitive internal roles are restricted to Backpack Works employees.

4. Authentication

- Platform authentication is handled by Supabase Auth.
- Customer integrations are connected via scoped OAuth permissions that customers can revoke at any time.
- MFA is enforced on internal systems that support it, and always for email, source control, and cloud consoles.

5. Provisioning & deprovisioning

- Access to internal and client systems is requested and approved before being granted, and recorded.
- Access is removed promptly (target: within one business day) upon role change or departure.

6. Access reviews

Access rights are reviewed at least quarterly for critical systems and corrected where needed.

7. Review

This policy is reviewed at least annually.